JULIA M. JAYNE (State Bar No. 202753)
ASHLEY RISER (State Bar No. 320538)
E-Mail: julia@jaynelawgroup.com
JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, CA 94607
Telephone: (415) 623-3600
Facsimile: (415) 623-3605

Attorneys for Defendant James Quach

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. XANTHE LAM, ALLEN LAM, JOHN CHAN, and JAMES QUACH, Defendants.	Case No. CR 18-00527 WHA **NOTICE OF MOTION AND MOTION TO DISMISS COUNTS 33-36 FOR FAILURE TO STATE AN OFFENSE** Date: December 17, 2019 Time: 2:00 p.m. Judge: Hon. William Alsup

TO THIS HONORABLE COURT, ASSISTANT UNITED STATES ATTORNEYS KYLE WALDINGER AND SHEILA ARMBRUST, AND ALL DEFENSE COUNSEL:

PLEASE TAKE NOTICE that on December 17, 2019 at 2:00 p.m.**,** or as soon thereafter as the matter may be heard before the above-entitled court, defendant JAMES QUACH, by counsel, will move and hereby does move the Court for an order dismissing Counts 33-36 of the indictment filed against him on the grounds that none of these counts adequately state an offense.

This motion is based on the papers, pleadings, and files of this action, the attached Memorandum of Points and Authorities, and on such oral and documentary evidence as may be presented at the time of the hearing.

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607

Dated: October 30, 2019

Respectfully submitted,

/s/

Julia Jayne
Ashley Riser
Attorneys for Defendant James Quach

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

On October 25, 2018, Xanthe Lam, Allen Lam, John Chan, and James Quach were indicted for alleged theft of trade secrets from Genentech, and violations of the Computer Crime and Abuse Act. Specifically, with respect to Count 33, the Indictment alleges that Ms. Lam and Mr. Quach violated Title 18 of the United States Code, section 1030(b), because they "did knowingly and willfully conspire and agree together, with each other, and with others known and unknown to the grand jury, to commit computer fraud and abuse, that is, to access protected computers without authorization and to exceed authorized access to protected computers…." Indictment, ¶ 28 (emphasis added).

Additionally, Counts 34-36 of the Indictment allege that Ms. Lam and Mr. Quach violated Title 18 of the United States Code, section 1030(a)(2)(C), because they "intentionally accessed a computer without authorization and exceeding authorized access..." Indictment, ¶ 33 (emphasis added). The same paragraph then states that "the defendants accessed Genentech's computer network without authorization." *Id.*

Xanthe Lam was an employee at Genentech with full access to Genentech's databases on the dates of the conduct alleged in Counts 33-36. It is alleged that Ms. Lam used her login credentials on her own computer on three dates, and allowed Mr. Quach to have access to Genentech's manufacturing, equipment, and facilities protocols. Counts 34-36, which allege violations of 18 U.S.C. § 1030(a)(2)(C), describe the offensive action as: "downloaded from Genentech's password-protected document repository." Indictment ¶ 26. There is no factual dispute that Ms. Lam was permitted to access the downloaded documents. Further, the indictment does not allege that Mr. Quach obtained Ms. Lam's login credentials and used them independently. Thus, the government only alleges misappropriation, which is not covered by the Computer Fraud and Abuse Act.

Mr. Quach therefore moves under Fed. R. Crim. Pro 12 to dismiss counts 33-36.

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607

ARGUMENT

I. COUNTS 33-36 MUST BE DISMISSED BECAUSE THE INDICTMENT ALLEGES MISAPPROPRIATION, WHICH IS NOT COVERED BY THE COMPUTER FRAUD AND ABUSE ACT.

As described above, the Indictment alleges one violation of conspiracy to violate the Computer Fraud and Abuse Act (CFAA) and three counts of violating the CFAA pursuant to 18 U.S.C. § 1030(a)(2)(C). That provision, in relevant part, makes it a crime for a person to "intentionally access a computer without authorization or exceed[ing] authorized access, and thereby obtains… information from any protected computer." The Indictment alleges that Xanthe Lam and James Quach "intentionally accessed a computer without authorization and exceeding authorized access" by downloading various documents from Genentech's password-protected document repository. Indictment at ¶ 26. There is no allegation that Mr. Quach hacked the Genentech system or ever possessed the login credentials. The Indictment alleges, in other words, that Ms. Lam and her purported co-conspirator, Mr. Quach, misappropriated information obtained from Genentech's database.

But the Indictment fails to state violations of the CFAA because the CFAA does not criminalize misappropriation. As a result, the four CFAA counts must be dismissed.

A. The Meaning of "Authorization"

Mr. Quach does not have notice of whether the government is alleging that he purportedly accessed Genentech's computer without authorization whatsoever, or whether he (and Ms. Lam) allegedly accessed the computer in excess of authorized access. The issue is addressed in Mr. Quach's corresponding Motion for Bill of Particulars.

For purposes of this motion, the core legal question centers around the meaning of authorization. This issue has been litigated in the Ninth Circuit, starting with *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012).

The CFAA's "general purpose is to punish hacking … not misappropriation of trade secrets." *Id*. The "1984 House Committee emphasized that 'Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the

conduct prohibited is analogous to … 'breaking and entering' rather than using a computer ... in committing the offense." *Shamrock Foods Co. v. Gas*t, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008), quoting H.R. Rep. No. 98–894, at 20 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3706.

As such, the Act criminalizes the unauthorized access of a protected computer. 18 U.S.C. § 1030(a)(1). The Act also criminalizes the access of a protected computer when that access "exceeds authorized access." *Id*. The Act defines "exceeds authorized access" as "access [to] a computer with authorization and [using] such access to obtain … information … that the accesser is not entitled … to obtain...." § 1030(e)(6). Yet the CFAA does not extend to violations of use restrictions and does not extend to misappropriation of information accessed with authorization. *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012); *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

B. The CFAA Counts (33-36)

Under the authority discussed above, all four CFAA counts against Mr. Quach must be dismissed.

Count 33 alleges Ms. Lam and Mr. Quach conspired to access protected computers without authorization and to exceed authorized access to protected computers. The "access" at issue pertains to the login credentials. But there can be no dispute that Ms. Lam was permitted to access the Genentech computer system, because she was an employee of Genentech without limitations on her access to the database.

Counts 34-36 allege substantive violations of 18 U.S.C. § 1030(a)(2)(C) on three different dates in July 2017. The "action" constituting the purported violation of the CFAA is the download from Genentech's password-protected document repository. Once again, Ms. Lam lawfully had the login credentials to the document repository. There is no allegation that she shared those login credentials with Mr. Quach and the Indictment is silent on what, if anything, was actually done with the downloaded documents. Further, any conduct with respect to what was done with the documents, and with whom they were shared, would constitute misappropriation, but not a violation of CFAA. The Ninth Circuit case law on this point is unambiguous. These counts

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607

therefore, on their face, likewise rest entirely on a misappropriation theory and therefore must be dismissed.

In sum, the Indictment does not allege that Ms. Lam or Mr. Quach "hacked" into any Genentech database, which is the heart of the CFAA. Ms. Lam could not hack her own computer or a database she was entitled to access. Nor did Mr. Quach "hack" or "break and enter" into the Genentech system because his alleged co-conspirator was an authorized user.

CONCLUSION

For the reasons stated above, this Court should dismiss Counts 33-36 of the Indictment.

Dated: October 30, 2019

Respectfully submitted,

/s/

Julia Jayne
Ashley Riser
Attorneys for Defendant James Quach

JAYNE LAW GROUP, P.C.
483 9th Street, Suite 200
Oakland, California 94607